

Office 365 Outbound Email Filtering

This topic outlines the steps to configure outbound mail routing from Office 365 through Cyren.

Prerequisites

By default, emails sent from Office 365 are DKIM signed, using the default domain:

[Customer].onmicrosoft.com

Cyren uses this information to validate the outbound email originated from the sender, and accepts the mail for outbound delivery.

The most reliable way a customer can check that this default DKIM signature is in place, is by inspecting a delivered outbound email, and ensuring that the `d=` field on the DKIM signature represents **[Customer].onmicrosoft.com**

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=[Customer].onmicrosoft.com; s=selector1-company-tld; h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-SenderADCheck;
```

It is possible to configure DKIM in Office 365 to use a different domain, or '(default signing domain)', however this configuration is not currently supported.

Cyren Cloud Security Configuration

In **Settings > Account** take a note of your Customer ID (**657nnn**) in this instance.

Account Information			
Customer Name:	<input type="text" value="Engineering"/>	Customer ID:	657nnn
Region Name:	US	Parent Partner Name:	Security
Default Time Zone supported for reports	<input type="text" value="US/Eastern (UTC -04:00) Eastern Time (US & Canada)"/>		

In **Settings>Email Services>Security>Outgoing Email Hosts** add an email host in the following format:

127.65.7n.nn

The second, third and fourth octet in the IP address added must represent your Customer ID.

Office 365 Configuration Steps

From the Office 365 Exchange Admin Center:

1. Select **Mail Flow>Connectors**, and add a new Connector.

2. Set **From:** to **Office 365**, and **To:** to **Partner Organization**, click **Next**.

New Connector - Google Chrome

Secure | https://outlook.office365.com/ecp/Connectors/ConnectorSelec...

Select your mail flow scenario

Specify your mail flow scenario, and we'll let you know if you need to set up a connector. [Learn more](#)

From:
Office 365

To:
Partner organization

Creating a connector is optional for this mail flow scenario. Create a connector only if you want to enhance security for the email messages sent between Office 365 and your partner organization or service provider. You can create multiple connectors for this scenario, each applying to different partner organizations or service providers. [Learn more about enhancing email security](#)

Next Cancel

3. Type in a connector name in the ***Name** field, for example, **Outbound Cyren Connector**.

It is mandatory to check the **Turn it on** checkbox.

New Connector - Google Chrome

Secure | https://outlook.office365.com/ecp/Connectors/OutboundConn...

New connector

This connector enforces routing and security restrictions for email messages sent from Office 365 to your partner organization or service provider.

*Name:

Description:

What do you want to do after connector is saved?
 Turn it on

4. Select **Only when email messages are sent to these domains** and add an * to the domain list, and click **Next**.

New Connector - Google Chrome

Secure | https://outlook.office365.com/ecp/Connectors/OutboundConn...

New connector

When do you want to use this connector?

Only when I have a transport rule set up that redirects messages to this connector

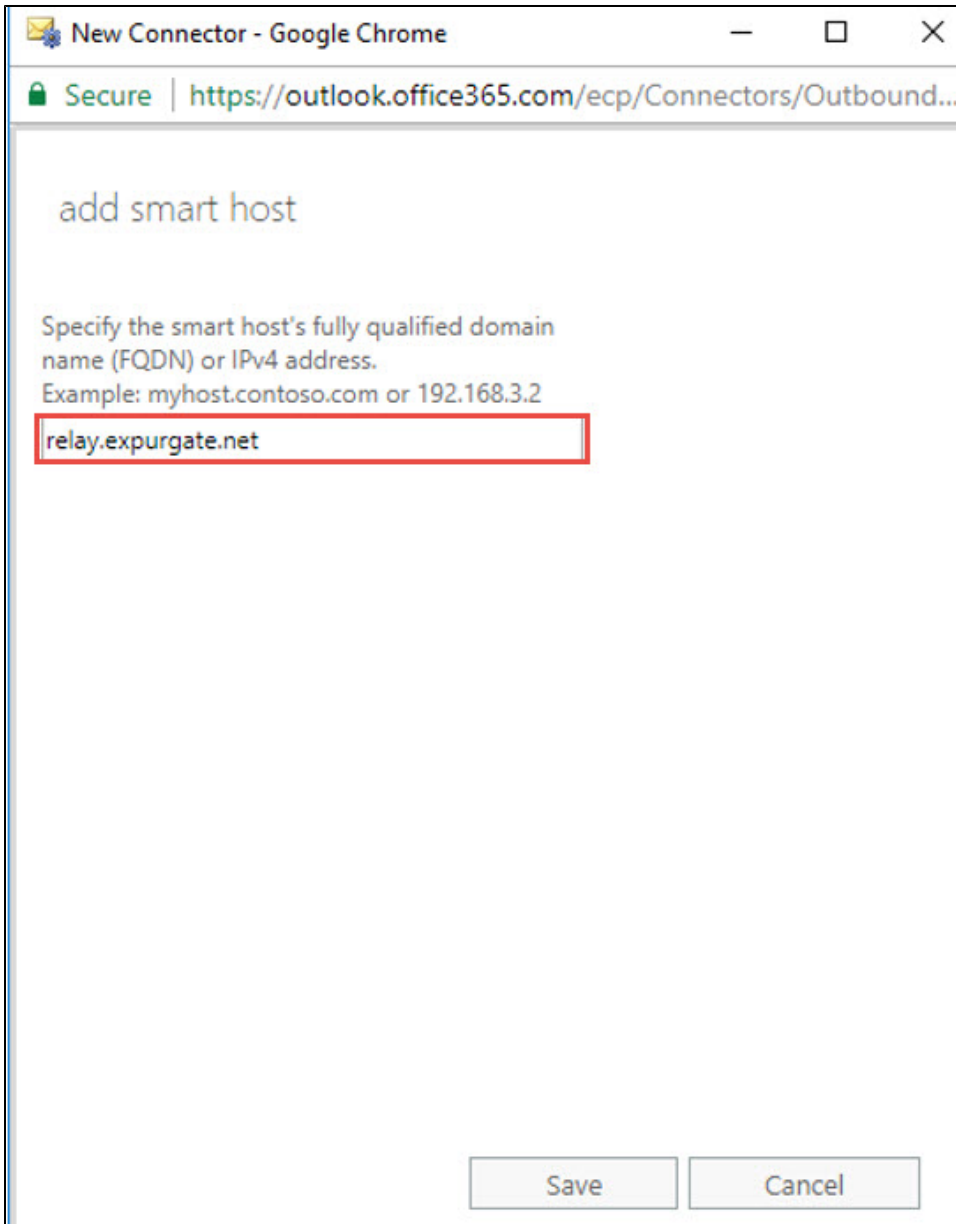
Only when email messages are sent to these domains

+ ✎ -

*

Back Next Cancel

5. Select **Route through these email smart hosts**, and add relay.expurgate.net to the list, and click **Next**.



The screenshot shows a browser window titled "New Connector - Google Chrome" with the address bar displaying "Secure | https://outlook.office365.com/ecp/Connectors/Outbound...". The main content area is titled "add smart host" and contains the following text: "Specify the smart host's fully qualified domain name (FQDN) or IPv4 address. Example: myhost.contoso.com or 192.168.3.2". A text input field below this text contains the value "relay.expurgate.net" and is highlighted with a red border. At the bottom of the dialog, there are two buttons: "Save" and "Cancel".

6. Select 'Always use TLS', and select 'Issued by a trusted certificate authority (CA)', click **Next**, and once again **Next**.

New Connector - Google Chrome

Secure | https://outlook.office365.com/ecp/Connectors/Outbound...

New connector

How should Office 365 connect to your partner organization's email server?

Always use Transport Layer Security (TLS) to secure the connection (recommended)
Connect only if the recipient's email server certificate matches this criteria

Any digital certificate, including self-signed certificates

Issued by a trusted certificate authority (CA)

And the subject name or subject alternative name (SAN) matches this domain name:
Example: contoso.com or *.contoso.com

TLS is a security protocol that helps to encrypt and deliver email messages securely so no one except the sender and recipient can access or tamper with the message. If you select this option, messages will be rejected if the TLS connection isn't successful.

Back Next Cancel

7. In the **Validate** screen, add an external email address and click **Validate**.

New Connector - Google Chrome

Secure | <https://outlook.office365.com/ecp/Connectors/Outbound...>

New connector

Validate this connector

We'll validate this connector for you to make sure it works as expected, but first you'll need to provide one or more email addresses so we can send a test message.

Specify an email address for your partner domain. You can add multiple addresses if your partner has more than one domain.

+ ✎ -

@gmail.com

Back Validate Cancel

Validation will fail if your domain (customer.onmicrosoft.com) has not been added to your Cyren account as a domain in **Settings > Email Services > Security > Email Gateway Settings**.